

A Robust Finite-Time Converse Theorem for Inductive Safety Certificates of Ordinary Differential Equations

Stefan Ratschan*,

Institute of Computer Science, Czech Academy of Sciences

February 8, 2017

Abstract

This paper is motivated by safety verification—the task of proving that a given system always stays in a given set of states considered to be safe. For proving this, one can use a certificate in the form of a set of states that (1) contains all initial states, that (2) is inductive (i.e., no solution leaves this set of states), and that (3) contains only safe states. The set of reachable states always forms such a certificate but for differential equations, this set is usually difficult to compute.

In this paper, we prove that for ordinary differential equations a certain *finite-time* reach set also forms such a certificate if certain boundedness and robustness assumptions hold. Moreover, this certificate is robust in the sense that it stays a certificate under small perturbations of the system.

1 Introduction

One important method used for formal safety verification is reach set computation: Compute the set of all states reachable by the system—if all those states are safe, then the system is safe. However, for non-linear ordinary differential equations, it is often difficult or even impossible [1] to compute the set of reachable states precisely. So, instead one over-approximates the set of states reachable in a certain finite time. If the resulting set is inductive (i.e., the system cannot leave this set) and all resulting states are safe, then the system is provably safe.

Experience has shown that this approach is often successful. In this paper we prove a theorem supporting this experience: We show that for systems given by ordinary differential equations, under the additional assumptions of robustness and boundedness of the set of safe states, a certain

*ORCID: 0000-0003-1710-1513

overapproximation of a finite time reach set is always a certificate for safety of the system.

We will now discuss related work: Inductivity is a principle that is used for safety verification throughout formal verification. However, its application to systems with infinitely many states is complicated by the fact that algorithms for reach set computation do not necessarily terminate due to non-convergence. This problem is usually handled using techniques such as widening [2]. In the case of differential equations the problem is exacerbated by the fact that reachability information can usually only be computed approximately. However, experience with verification tools [7, 5] has shown that such approximations often help convergence, in a similar way as widening.

Algorithms that have been used for proving decidability of safety verification under robustness assumptions (this is also known as quasi-decidability), construct such certificates [4, 3, 15], but the certificates are the side-product of a complex algorithmic process and are not of a simple form as the result of this paper.

A similar object that is often used for safety verification of continuous systems are barrier certificates [12, 17, 6], where derivative information is used for getting rid of reach set computation. Here, there are also converse theorems showing the existence of such barrier-certificates. However, those results are either restricted to systems where certain Lyapunov-like functions exist [13, 14], or to Morse-Smale vector fields [18].

The research published in this paper was supported by GAČR grant 15-14484S and by the long-term strategic development financing of the Institute of Computer Science of the Czech Academy of Sciences (RVO:67985807). We thank Peter Franek for important feedback throughout the work on this paper.

2 The Problem

Definition 1. *A safety verification problem is a triple (f, I, S) that consists of*

- *a continuous time dynamical system $\dot{x} = f(x)$, with $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$, where f is Lipschitz continuous,*
- *a set of states I that we will call the initial states of the safety verification problem,*
- *and set of states S that we will call the safe states of the safety verification problem.*

Definition 2. *For a Lipschitz continuous $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$, $t \in \mathbb{R}^{\geq 0}$, we denote the state that system $\dot{x} = f(x)$ reaches after time t from x by $\tau_f(x, t)$.*

Based on this we introduce the following notation for sets of reachable states:

Definition 3. For a Lipschitz continuous $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$, for sets $X \subseteq \mathbb{R}^n$ and $T \subseteq \mathbb{R}^{\geq 0}$, $R_f^T(X) := \{\tau_f(x, t) \mid t \in T, x \in X\}$. For $t \in \mathbb{R}^{\geq 0}$, $R_f^t(X) := R_f^{\{t\}}(X)$, and $R_f(X) := R_f^{\mathbb{R}^{\geq 0}}(X)$.

Definition 4. A safety verification problem (f, I, S) is safe iff $R_f(I) \subseteq S$.

Definition 5. A set $V \subseteq \mathbb{R}^n$ is a safety certificate of a safety verification problem (f, I, S) iff

- $I \subseteq V$
- $R_f(V) \subseteq V$
- $V \subseteq S$

A set that fulfills the first two conditions is also called *inductive invariant* by the verification community, and a *positively invariant set* by the dynamical systems literature [10, 8].

Safety certificates serve as a proof of safety:

Property 1. If a safety verification problem (f, I, S) has a safety certificate, then it is safe.

Safety certificates are also complete, that is, there is a converse of Property 1:

Property 2. If a safety verification problem (f, I, S) is safe, then it has a safety certificate, $R^{[0, \infty]}(I)$.

However, there are two problems with applying this property in safety verification:

- It uses the infinity symbol ∞ which can make computation of the set $R^{[0, \infty]}(I)$ difficult.
- It does not take into account approximation.

We will now extend some of the definitions above to take into account deviations from nominal behavior. For measuring such deviations we will use the Euclidean norm, denoted by $\|\cdot\|$.

Definition 6. A function $x : \mathbb{R}^{\geq 0} \rightarrow \mathbb{R}^n$ is an ε -solution of f iff for all $t \geq 0$, $\|f(x(t)) - \dot{x}(t)\| \leq \varepsilon$.

We use the following robust versions of the reach sets introduced in Definition 3:

Definition 7. For a Lipschitz continuous $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$, for sets $X \subseteq \mathbb{R}^n$ and $T \subseteq \mathbb{R}^{\geq 0}$, $R_{f, \varepsilon}^T(X) := \{x(t) \mid t \in T, x \text{ is an } \varepsilon\text{-solution of } f \text{ with } x(0) \in X\}$, $R_{f, \varepsilon}^t(X) := R_{f, \varepsilon}^{\{t\}}(X)$, $R_{f, \varepsilon}(X) = R_{f, \varepsilon}^{\mathbb{R}^{\geq 0}}(X)$.

Here, if clear from the context, we will drop the subscript f .

Also Definition 4 has a robust version:

Definition 8. A safety verification problem (f, I, S) is robustly safe iff there is an $\varepsilon > 0$ such that $R_{f,\varepsilon}(I) \subseteq S$. We will call an $\varepsilon > 0$ fulfilling this property a robustness margin of (f, I, S) .

Finally, we provide a robust version of Definition 5:

Definition 9. A set $V \subseteq \mathbb{R}^n$ is an ε -robust safety certificate of a safety verification problem (f, I, S) iff

- $I \subseteq V$
- $R_{f,\varepsilon}(V) \subseteq V$
- $V \subseteq S$

We call a safety certificate V robust if there is an $\varepsilon > 0$ such that V is a ε -robust safety certificate.

The main theorem of this paper is a converse of Property 1 that is based on a finite time each set, and that is robust.

Theorem 1. If a safety verification problem (f, I, S) is robustly safe with robustness margin ε and the set of safe states S is bounded, then for all $\Delta > 0$ there is a $t \geq 0$ such that $R_{f,\frac{\varepsilon}{2}}^{[0,\Delta]}(R_{f,\varepsilon}^{[0,t]}(I))$ is an $\frac{\varepsilon}{2}$ -robust safety certificate.

3 Proof

We will now translate a standard result on controllability to our context, ensuring that every point that is ε -reachable has a neighborhood of $\hat{\varepsilon}$ -reachable points with $\hat{\varepsilon} > \varepsilon$. Here we denote by $N_\delta(p)$ the δ -neighborhood $\{p' \mid \|p - p'\| < \delta\}$ of p .

Property 3. For every Lipschitz continuous $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$, $\varepsilon, \hat{\varepsilon}$ with $\hat{\varepsilon} > \varepsilon \geq 0$, $\Delta > 0$, $p \in \mathbb{R}^n$ and p' such that $p' \in R_{f,\varepsilon}^\Delta(\{p\})$ there is a $\delta > 0$ such that

$$N_\delta(p') \subseteq R_{f,\hat{\varepsilon}}^\Delta(\{p\}).$$

The usual proof of this property [11, Proposition 3.3], [16, Proposition 11.2] uses the inverse function theorem to map each point in the neighborhood of p' to controls of bounded norm that steer the system into this point. Due to a version of the inverse function theorem [9] that bounds the size of this neighborhood from below based on a Lipschitz constant for the derivative of the given function, the size δ of the neighborhood in Property 3 can be bounded from below over all elements p and p' of a compact set:

Lemma 1. *For every Lipschitz continuous $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$, and compact set $\Omega \subseteq \mathbb{R}^n$, for every $\varepsilon > 0$, $\Delta > 0$ there is a $\delta > 0$ such that for all $p, p' \in \Omega$ such that $p' \in R_{f, \frac{\varepsilon}{2}}^\Delta(\{p\})$,*

$$N_\delta(p') \subseteq R_{f, \varepsilon}^\Delta(\{p\}).$$

We will now turn to the proof of the main theorem. It extends a technique introduced by M. Fränzle [4], that he originally used for constructing a safety certificate for hybrid systems with polynomial flow: Take the bloated finite-time reach set $R_{f, \varepsilon}^{[0, t]}(I)$, and show that the original dynamics is shrinking on it if the bloated reach set does not grow beyond the set of safe states S . However, here we have additional complications: First, our flow is, in general, not polynomial (note that even linear ODEs usually have a non-polynomial flow), and second, we are not satisfied with a safety certificate, but we want a *robust* safety certificate.

Proof. We assume that (f, I, S) is robustly safe with robustness margin $\varepsilon > 0$, and that the set of safe states S is bounded. We derive a contradiction from the additional assumption that there is a $\Delta > 0$ such that for all $t \geq 0$ $R_{f, \frac{\varepsilon}{2}}^{[0, \Delta]}(R_{f, \varepsilon}^{[0, t]}(I))$ is no $\frac{\varepsilon}{2}$ -robust safety certificate. In the following, let $\Delta > 0$ be an arbitrary constant fulfilling this property.

We now observe that for every $t \geq 0$, $R_{f, \varepsilon}^{[0, t]}(I)$ contains a point ξ such that there is a $\xi' \in R_{f, \frac{\varepsilon}{2}}^{[\Delta, \infty]}(\{\xi\})$ s.t. $\xi' \notin R_{f, \varepsilon}^{[0, t]}(I)$. If this would not be the case, then there would exist a $t \geq 0$, such that for all $\xi \in R_{f, \varepsilon}^{[0, t]}(I)$, for all $\xi' \in R_{f, \frac{\varepsilon}{2}}^{[\Delta, \infty]}(\{\xi\})$, $\xi' \in R_{f, \varepsilon}^{[0, t]}(I)$. This means that no $\frac{\varepsilon}{2}$ -solution would leave $R_{f, \frac{\varepsilon}{2}}^{[0, \Delta]}(R_{f, \varepsilon}^{[0, t]}(I))$. Hence $R_{f, \frac{\varepsilon}{2}}^{[0, \Delta]}(R_{f, \varepsilon}^{[0, t]}(I))$ would be a $\frac{\varepsilon}{2}$ -robust safety certificate, which would be in contradiction to the assumption above.

We now derive a contradiction from the above by constructing an infinite sequence of points p_1, \dots , such that

- for every i , $p_i \in R_{f, \varepsilon}^{[0, \infty]}(I)$, and
- for every i, j , $i \neq j$, we have $\|p_j - p_i\| > \delta$,

with δ being a positive real number. This implies that the maximal distance of two points in the sequence grows over all bounds. Since the set of safe states S is bounded, this is a contradiction to the fact that (f, I, S) is robustly safe.

We ensure the second property (sufficient distance of points) by constructing at the same time a sequence t_1, \dots , such that, for all i ,

- every point not ε -reachable in time t_i , that is, every point not in $R_{f, \varepsilon}^{[0, t_i]}(I)$ has distance at least δ from every point p_1, \dots, p_i (in Figure 1, the δ -balls around p_i are inside of the reach sets $R_{f, \varepsilon}^{[0, t_i]}(I)$).

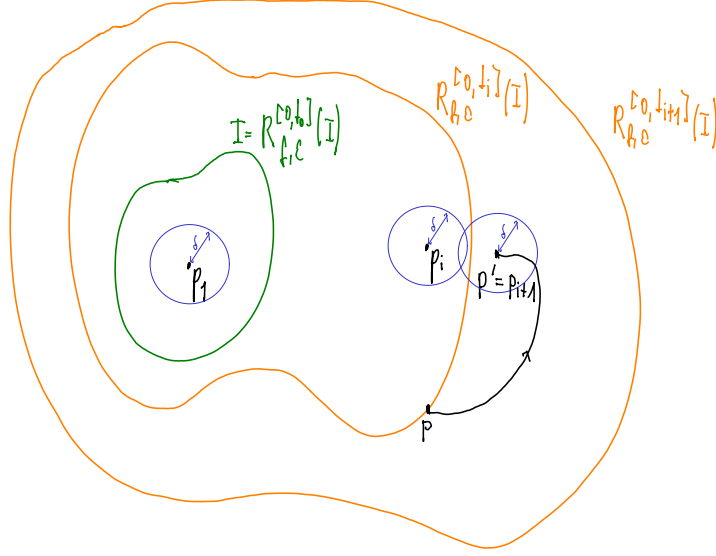


Figure 1: Proof Intuition

- p_{i+1} is not ϵ -reachable in time t_i , that is, $p_{i+1} \notin R_{f, \epsilon}^{[0, t_i]}(I)$ (in Figure 1, the points $p' = p_{i+1}$ are outside of the reach sets $R_{f, \epsilon}^{[0, t_i]}(I)$).

It remains to construct the sequences p_1, \dots , and t_1, \dots , in such a way. Due to the Heine-Borel theorem, the closure of S is compact. So we can apply Lemma 1: Let δ be as given by Lemma 1 for Ω being the closure $cl(S)$ of the set of safe states S . So for all $p, p' \in cl(S)$ with $p' \in R_{f, \frac{\epsilon}{2}}^{\Delta}(\{p\})$, $N_{\delta}(p') \subseteq R_{f, \epsilon}^{\Delta}(\{p\})$.

Let i be an arbitrary, but fixed natural number, and assume that the above properties hold for p_1, \dots, p_i and t_1, \dots, t_i . We construct p_{i+1}, t_{i+1} together with a proof that the above properties hold for them.

Let $p \in R_{f, \epsilon}^{[0, t_i]}(I)$, $p' \in R_{f, \frac{\epsilon}{2}}^{[\Delta, \infty]}(\{p\})$, $p' \notin R_{f, \epsilon}^{[0, t_i]}(I)$, as ensured by the observation at the beginning of the proof. By Lemma 1, every point in the δ -neighborhood of p' is reachable in time Δ from $p \in R_{f, \epsilon}^{[0, t_i]}(I)$ with ϵ -perturbed dynamics.

So we choose $p_{i+1} = p'$, $t_{i+1} = t_i + \Delta$. Then $p_{i+1} \notin R_{f, \epsilon}^{[0, t_i]}(I)$, and hence has distance at least δ from p_1, \dots, p_i . Moreover, every point not reachable in time t_{i+1} again has distance at least δ from p_1, \dots, p_{i+1} .

We choose $t_1 = 0$ and p_1 an initial point that has distance at least δ from the boundary of the set of initial points I (the case where such a point does not exist can be easily handled by shifting the sequence).

We now have an infinite sequence of points p_1, \dots , such that

- for every i , $p_i \in R_{f, \epsilon}^{[0, \infty]}(I)$, and

- for every $i, j, i \neq j$, we have $\|p_j - p_i\| > \delta$.

This is a contradiction to the fact that (f, I, S) is robustly safe with robustness margin ε and S is bounded. □

The proof also explains, why the theorem requires Δ to be strictly greater than zero: Due to this, we have a strictly positive lower bound on the length of the solution leading from p to $p' = p_{i+1}$ outside of the set of points reachable in time t_i . This allows us to use Lemma 1 to construct a δ -neighborhood of $p' = p_{i+1}$ reachable in time t_{i+1} .

4 Conclusion

We have shown that every robust safety verification problem with a bounded set of safe states has a robust safety verification certificate formed by a finite time reach set. At this point, the theorem is purely theoretical: It gives a general justification for the usage of over-approximations of finite-time reach sets in safety verification, but does not result in a concrete algorithm. It would be interesting to see whether such converse theorems can be used for improving concrete safety verification algorithms.

References

- [1] O. Bournez and M. L. Campagnolo. A survey on continuous time computations. In S. Cooper, B. Lwe, and A. Sorbi, editors, *New Computational Paradigms*, pages 383–423. Springer New York, 2008.
- [2] P. Cousot and R. Cousot. Abstract interpretation: A unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *Fourth ACM Symposium on Principles of Programming Languages*, pages 238–252, 1977.
- [3] W. Damm, G. Pinto, and S. Ratschan. Guaranteed termination in the verification of LTL properties of non-linear robust discrete time hybrid systems. *International Journal of Foundations of Computer Science (IJFCS)*, 18(1):63–86, 2007.
- [4] M. Fränzle. Analysis of hybrid systems: An ounce of realism can save an infinity of states. In J. Flum and M. Rodriguez-Artalejo, editors, *Computer Science Logic (CSL'99)*, number 1683 in LNCS. Springer, 1999.
- [5] G. Frehse. Phaver: algorithmic verification of hybrid systems past HyTech. *International Journal on Software Tools for Technology Transfer (STTT)*, 10(3):263–279, 2008.

- [6] K. Ghorbal, A. Sogokon, and A. Platzer. A hierarchy of proof rules for checking positive invariance of algebraic and semi-algebraic sets. *Computer Languages, Systems & Structures*, 47:19–43, 2017.
- [7] T. A. Henzinger, P.-H. Ho, and H. Wong-Toi. HYTECH: a model checker for hybrid systems. *International Journal on Software Tools for Technology Transfer (STTT)*, 1:110–122, 1997.
- [8] M. W. Hirsch, S. Smale, and R. L. Devaney. *Differential Equations, Dynamical Systems, and an Introduction to Chaos*. Academic Press, 2nd edition edition, 2003.
- [9] J. H. Hubbard and B. B. Hubbard. *Vector Calculus, Linear Algebra, And Differential Forms*. Matrix Editions, 2001.
- [10] H. K. Khalil. *Nonlinear Systems*. Prentice Hall, 3rd edition, 2002.
- [11] H. Nijmeijer and A. Van der Schaft. *Nonlinear dynamical control systems*. Springer-Verlag New York, 1990.
- [12] S. Prajna and A. Jadbabaie. Safety verification of hybrid systems using barrier certificates. In R. Alur and G. J. Pappas, editors, *HSCC’04*, number 2993 in LNCS. Springer, 2004.
- [13] S. Prajna and A. Rantzer. On the necessity of barrier certificates. In *Proceedings of the IFAC World Congress*, Prague, Czech Republic, July 2005.
- [14] S. Prajna and A. Rantzer. Convex programs for temporal verification of nonlinear dynamical systems. *SIAM Journal on Control and Optimization*, 46(3):999–1021, 2007.
- [15] S. Ratschan. Safety verification of non-linear hybrid systems is quasi-decidable. *Formal Methods in System Design*, 44(1):71–90, 2014.
- [16] S. Sastry. *Nonlinear systems: analysis, stability, and control*. Springer-Verlag New York, 1999.
- [17] A. Taly and A. Tiwari. Deductive verification of continuous dynamical systems. In R. Kannan and K. N. Kumar, editors, *IARCS Annual Conf. on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2009)*, volume 4 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 383–394, Dagstuhl, Germany, 2009.
- [18] R. Wisniewski and C. Sloth. Converse barrier certificate theorems. *IEEE Transactions on Automatic Control*, 61(5):1356–1361, 2016.